IN THE CLAIMS

Upon entry of the present amendment, the status of the claims will be as is shown below. This listing of claims replaces all previous versions and listings of claims in the present application.

1. (Original) A method for providing secure communications through a communications network comprising ATM channels and TDM channels, the communications network including at least one closed user group of network elements configured to communicate with only other network elements in the closed user group, the method comprising:

receiving a connection setup request at an ingress ATM switch, via a UNI attached to the ATM switch, in response to a call initiated through a TDM channel, the UNI interfacing a first network element of the closed user group with the ATM switch;

verifying that an ATM End System Address (AESA) contained in calling party information of the connection setup request is consistent with the attached UNI; and

establishing a connection with at least a second network element of the closed user group through an egress ATM switch in the communications network when the AESA is consistent with the attached UNI.

2. (Original) The method for providing secure communications through the communications network, according to claim 1, further comprising:

denying access to the second network element of the closed user group when the AESA is not consistent with the attached UNI.

3. (Original) The method for providing secure communications through the communications network, according to claim 2, further comprising:

sending an alarm to an ATM element management system when the AESA is not consistent with the attached UNI.

4. (Original) The method for providing secure communications through the communications network, according to claim 1, in which the attached UNI comprises a physical port/UNI.

5. (Original) The method for providing secure communications through the communications network, according to claim 1, in which the attached UNI comprises a virtual UNI.

6. (Original) The method for providing secure communications through the communications network, according to claim 1, in which verifying the AESA comprises comparing a network prefix of the AESA to a network prefix previously assigned to the UNI.

7. (Original) The method for providing secure communications through the communications network, according to claim 1, further comprising:

establishing a membership list at an ATM element management system identifying each network element that is part of the closed user group; and

verifying that each of the first network element and the second network element belongs to the closed user group using the membership list, prior to establishing the connection.

8. (Previously presented) The method for providing secure communications through the communications network, according to claim 1, in which the first network element and the second network element comprise trunk interworking function (T-IWF) devices configured to convert between voice streams from TDM channels to cell streams from ATM channels.

9. (Original) The method for providing secure communications through the communications network, according to claim 1, in which the connection comprises a switched virtual circuit connection.

10. (Currently amended) A system for enforcing switched virtual circuit (SVC) access restrictions across an Asynchronous Transfer Mode (ATM) distributed virtual tandem switching system based on closed user

groups of network elements in a communications network, the system comprising:

a plurality of trunk interworking function (T-IWF) devices in the communications network, configured to convert between voice streams from TDM communications channels to cell streams from ATM communications channels, a first one of the plurality of T-IWF devices receiving a call via at least one TDM communications channel from an end office;

a centralized control and signaling interworking function (CS-IWF) device that receives narrowband signaling data relating to routing the call, the CS-IWF device converting the narrowband signaling data to broadband signaling data to control the call through an ATM switching network and determining that the call is directed to a second one of the plurality of T-IWF devices, the plurality of T-IWF devices and the CS-IWF device being in a previously established closed user group; ~~and~~

an ATM switch in the ATM switching network that receives a request from one of the CS-IWF device and the T-IWF devices to establish an SVC connection of the call over the ATM switching network; and

an ATM element management system that stores a list of network elements in the closed user group, including the CS-IWF device and the plurality of T-IWF devices, the determination of whether the CS-IWF device, the first T-IWF device and the second T-IWF device are in the closed user group being based on the list of network elements;

wherein the ATM switch establishes the SVC connection over the ATM switching network, enabling broadband communication between the first T-IWF device and the second T-IWF device, when the CS-IWF device, the first T-IWF device and the second T-IWF device are determined to be in the closed user group; ~~and~~

wherein the ATM switch does not establish the SVC connection over the ATM switching network when at least one of the CS-IWF device, the first T-IWF device and the second T-IWF device is determined not to be in the closed user group; and

wherein the ATM switch verifies that an ATM End System Address (AESA) contained in calling party information in the request from the CS-IWF device is consistent with a user-to-network interface between the first T-IWF device and the ATM switch, the ATM switch rejecting the request to establish the SVC connection over the ATM switching network when the AESA is not consistent with the UNI.

11. – 12. (Canceled)

13. (Currently amended) The system for enforcing SVC access restrictions according to claim 10 ~~12~~, in which the ATM switch sends an alarm to the ATM element management system when the AESA is not consistent with the UNI.

14. (Currently amended) The system for enforcing SVC access restrictions according to claim 10 ~~12~~, in which the UNI comprises a physical port/UNI.

15. (Currently amended) The system for enforcing SVC access restrictions according to claim 10 ~~12~~, in which the UNI comprises a virtual UNI.

Claims 16 - 27 (Cancelled)